⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭63－240629

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和63年(1988)10月6日
G 06 F 9/06	330	A－7361－5B	
12/14	320	B－7737－5B	
G 09 C 1/00	310	7368－5B	審査請求　有　請求項の数 4　(全8頁)

⑤4発明の名称　プログラムを機密保護し且つ機密保護されたプログラムを保全制御する方法

⑳特　願　昭63－40545
㉒出　願　昭63(1988)2月23日

優先権主張　㉜1987年2月23日㉝西ドイツ(DE)㉞P3705736.7

⑦2発明者　ベルナー・バウリーニ　ドイツ連邦共和国4796ザルツコツテン、ヴアルトベーク15ベー

⑦2発明者　ディーター・ベツセル　ドイツ連邦共和国4795デルブルツク、ポールスシユトセーセ21

⑦1出願人　ニクスドルフ・コンピユータ・アクチエンゲゼルシヤフト　ドイツ連邦共和国4790パーダーボーン、フユルステンアレー　7

⑦4代理人　弁理士　秋元　輝雄　外1名

明　細　書

1．発明の名称

プログラムを機密保護し且つ機密保護されたプログラムを保全制御する方法

2．特許請求の範囲

(1)　データ処理装置のシステム記憶装置に記憶されているプログラムを機密保護し且つ機密保護されたプログラムを保全制御する方法において、少なくともシステム始動を生じさせるプログラムは、それぞれ対称暗号アルゴリズムに従い、読出し保護状態で記憶されている秘密キーを使用して、検査暗号形成のために暗号化され、検査暗号はシステム記憶装置に記憶されることと、データ処理装置のシステム始動に伴なう保全制御のために、プログラムの連続する再度のそのような暗号化と、それぞれ、そのように形成された検査暗号と対応する記憶された検査暗号との比較とが開始され、比較の結果が否定である場合は、それぞれ後続するシステム始動ステップ又はプログラムの活動化を阻止可能であることを特徴とする方法。

(2)　システム始動の開始を生じさせるプログラム(事前ローダプログラム)の第1の検査暗号は読出し保護状態で記憶されることを特徴とする特許請求の範囲第1項記載の方法。

(3)　アルゴリズムとしてDESアルゴリズムが使用されることを特徴とする特許請求の範囲第1項又は第2項記載の方法。

(4)　スーパーバイザリーコンピュータ及びオブジェクトコンピュータから構成されるコンピュータネットワークにおいてプログラムを機密保護するために、オブジェクトコンピュータのシステムサポータに関する第1に挙げたキーがスーパーバイザリーコンピュータで実行されることと、保全制御のための再度の暗号化は、それぞれのオブジェクトコンピュータにおいて、同じ読出し保護状態で記憶された秘密キーを使用して、システム始動手順に伴なって自動的に実行されることを特徴とする特許請求の範囲第

1項から第3項のいずれか1項に記載の方法。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、データ処理装置のシステム記憶装置に記憶されているプログラムを変更に対して機密保持し且つ機密保持されたプログラムを保全制御する方法に関する。

〔従来の技術及び発明が解決しようとする問題点〕

データ処理装置及びそれらと共に構成されるコンピュータシステムにおいては、制御及び応用の目的に使用されるプログラム、すなわち、オペレーションシステムと、アプリケーションシステムとから構成されるプログラムシステムが、たとえば磁気ディスク等のシステム記憶装置に記憶されている。データ処理装置が動作するとき、オペレーティングシステムの枠内でデータ処理装置の動作プロセスを制御すると共に、アプリケーションシステムの枠内でユーザーにより提示されたデータ処理タスクを実行するために、プログラムは作業用記憶装置にロードされ、処理される。

データ処理装置と共に、個々のコンピュータが互いに通信し合うコンピュータネットワークが開発されている。この場合に自動的に進行する情報交換は、特に銀行業務、保険業務、商取引き又は行政等の適用領域では詐欺的操作から機密保護されなければならない。そのような操作はコンピュータの面にも及び、コンピュータが望ましくない別の命令を実行したり、実行する命令の数が規定より少なくなったりすることや、命令の変更が行なわれることも起こり、その結果、個人に関連するデータが悪用され、誤って処理され、転用される、又はコンピュータ出力が権限のない者の手に渡って悪用される、あるいはコンピュータネットワークのユーザー又は第三者に対してその他の損害を与えるといった事態も起こりかねない。

コンピュータネットワークのユーザーにとっては、操作されたプログラムを認識した上で、相応する修正措置により保全性を確保することは非常に困難であるので、プログラムの操作を自動的に認識し、操作されたプログラムの実行を同様に自動的に阻止することを可能にすべきであろう。しかしながら、プログラムを機密保護する従来の方法としては、無許可の複写を阻止し、そのために、そのようなプログラムの実行のための特別なプロセッサを必要とする暗号化を適用する方法が知られているにすぎない。このような機密保護手段はプログラムの無許可の経済的利用及び転用を阻止すべきものであるが、コンピュータネットワーク内におけるプログラムへの操作を認識し、誤ったプログラム実行を阻止することはできない。また、無許可の者による操作に対してある程度の保護を達成するために、パスワード又はユーザーカタログの使用、データの秘密保持、あるいは特別のスイッチ又はキーを介した許可授与等の物理的措置により動作手段制御及びアクセス制御を行なうことも可能である。しかし、これらの方法は、プログラマー又はこれと同等の資格をもつ者がコンピュータネットワークをアクセスしようとした場合には、相当に無力なものになってしまう。すなわち、その場合には、特殊な専門知識に基づいて、上述のような種類の保護措置が講じられているにもかかわらず、プログラムを操作することが可能なのである。

本発明の目的は、データ処理装置において、プログラムに対する操作をシステム性能を大きくそこなうことなく自動的に認識し且つ操作されたプログラムの有効化を自動的に阻止することを可能にする方法を提案することである。

〔問題点を解決するための手段〕

本発明によれば、上記の目的は、冒頭に述べた種類の方法について、少なくともシステム始動を生じさせるプログラムが、それぞれ対称暗号アルゴリズムに従い、読出し保護状態で記憶されている秘密キーを使用して、検査暗号形成のために暗号化され、検査暗号はシステム記憶装置に記憶されることと、データ処理装置のシステム始動に伴なう保全制御のために、プログラムの連続する再度のそのような暗号化と、それぞれ、そのように形成された検査暗号と対応する記憶された検査暗号との比較が開始され、比較の結果が否定である

場合は、それぞれ後続するシステム始動ステップ又はプログラムの活動化を阻止可能であることにより達成される。

本発明により、データ処理装置のプログラムシステム全体、すなわち、オペレーティングシステムとアプリケーションシステムの双方における操作が自動的に認識されるようになり、既にシステム始動の段階で、操作の認識に応じて直ちに動作を中断させることができる。これにより、プログラムの「封印」、すなわち、システム記憶装置又はシステムサポータの封印という効果が得られ、この効果はデータ処理装置のシステム始動時に既に実行可能である保全制御によって発揮される。プログラムの機密保護のために、システム記憶装置は検査暗号の形をとる付加情報を記憶しているが、それらの検査暗号は、秘密キーを基礎として実行される暗号化ステップの結果として形成される。スーパーバイザリーコンピュータと、複数のオブジェクトコンピュータとを有するコンピュータネットワークにおいては、それぞれのオブジェクトコンピュータに対するシステムサポータはスーパーバイザリーコンピュータでこのようにして封印され、その際、検査暗号は、システムサポータに記憶されていてロード可能であり且つ応用システムのプロセス遂行には不可欠である全てのプログラムに対して論理封印として作用することができる。これは、コンピュータの動作中に記憶装置に常駐しているオペレーティングシステムのプログラムと、ロードライブラリーに読出可能な形態で記憶されている全てのプログラムを指す。この封印のために、読出し保護状態で記憶されている秘密キーが使用されるので、プログラムに対する無許可の操作のたびに、オブジェクトコンピュータにおいて同一の秘密キーを使用して、検査暗号の形成を伴ないながら、操作された各々のプログラムの再度の暗号化を実行する保全制御に際し、本発明に従って実施されるべき比較ステップで操作されたプログラムについて実行された暗号化により得られた検査暗号と、スーパーバイザリーコンピュータにおいて操作されないプログラムについて得られた検査暗号との間に不一致が生じるため、そこで、誤り信号が発生される。次に、この誤り信号を利用して、後続するプログラムの活用化を自動的に阻止することができる。

暗号化は対称暗号アルゴリズムを使用して実行される。公知のように、この暗号化原理は解読に対して非常に高い機密保護レベルを示す。公知の実施形態はＤＥＳアルゴリズムである(DES＝DATA Encryption Standard 、データ通信用暗号標準)。暗号化されたテキストの解読は、クリアテキストの暗号化とは全く逆の順序で行なわれる。このため、対称法と呼ばれている。このアルゴリズムの高い機密保護レベルはその数学的特性によるものであり、クリアテキストの知識と、付随するキーテキストの知識をもってしても、秘密キーを見出すのは容易なことではない。しかしながら、本発明の範囲内では、ＤＥＳアルゴリズムはデータの暗号化ではなく、プログラムの暗号化に際しての検査総和の取出しのために適用される。

暗号化に使用されるキーの読出し保護状態での記憶もそれ自体知られており、そのために、特別の機密保護コンポーネントがコンピュータネットワークの各コンピュータに具備されている。この機密保護コンポーネントは、使用されるキーを物理的にアクセス不可能な形態で記憶する記憶装置を含むことができる。さらに、機密保護コンポーネントは、本発明により達成される機密保護効果を一段と向上させることができる他のハードウェア機能ユニットを含んでいて良いことも知られている。

本発明による方法は、プログラムシステムの経過に相応して、一連の互いに連続する暗号化ステップ又は制御ステップで実行されるので、システム始動のスタートを生じさせるプログラム、いわゆる事前ローダプログラムの第１の検査暗号が読出し保護状態で記憶されれば、無許可のプログラム操作の影響に対して本発明により達成される機密保護レベルをさらに高めることができる。この付加的手段は、制御シーケンスで発生する第１の検査暗号を知ることを妨げるので、この検査暗

号を使用して、事前ローダプログラムの暗号化の基礎ともなった秘密キーを探り出そうとする試みを不可能にする。これにより、保全制御の枠内で進行する第１の検査プロセスは無許可のアクセス及び変更に対して絶対的に保護された状態となる。

〔実　施　例〕

以下、添付の図面を参照して本発明を詳細に説明する。

以下に説明されるのは、本発明によるプログラムを機密保護する方法をスーパーバイザリーコンピュータ及びオブジェクトコンピュータを伴なって実際に適用した場合に、その方法がいかにして実施されるかということである。この場合、一般に、スーパーバイザリーコンピュータには、オブジェクトコンピュータの動作開始のために稼動可能なシステムサポータが検査暗号の形態をとる付加情報と共に備えられている。これらの検査暗号は、機密保護コンポーネントに記憶された秘密キーを適用することによって実行される複数の暗号化ステップから得られるもので、システムサポータに記憶されたプログラムはそれらの暗号化ステップの下に順次置かれる。検査暗号は、オブジェクトコンピュータのシステムサポータに記憶されていてローディング可能であり且つ応用システムのプロセス進行には不可欠である全てのプログラムに対して、論理的な封印となる。さらに、この場合、機密保護コンポーネントに読取り不可能なように記憶されるスタート手順のための検査暗号が発生される。暗号化ステップに関する秘密キーはアクセス不可能であるため、他の全ての検査暗号はシステムサポータにアクセス可能及び読取り可能に記憶されることができる。オブジェクトコンピュータの機密保護コンポーネントは、これに記憶されているキーが、機密保護コンポーネントに供給された基準検査暗号との比較を同時に実行する場合にその比較の対象となる検査暗号を計算するためにのみ使用されるように動作するので、機密保護コンポーネントはその結果として検査暗号を出力することはできず、計算された検査暗号が基準検査暗号と一致するか否かに関するイエス／ノーのステートメントのみを出力する。すなわち、オブジェクトコンピュータシステムにおいては、秘密キーを知らずに許可なくＰＺ検査暗号を計算することは不可能である。

スーパーバイザリーコンピュータに上述のような方式により付加情報を伴なうシステムサポータが設けられた後、このシステムサポータをオブジェクトコンピュータに導入することができる。オブジェクトコンピュータの動作開始に際して、保全制御は、時間的に見て応用動作の前に進行しているシステム始動手順の中で自動的に実行される。その場合、複数の検査ステップが発生することになるが、それぞれの検査ステップは、その実行コードが先の検査ステップのときと変わらないと証明されたときに始めて開始される。

第１の検査ステップは事前ロードプログラムから開始され、機密保護コンポーネントにおいて実行される。従って、この論理は物理的に自由にアクセス可能ではない。事前ロードプログラムが物理的に影響を受けると、すなわち変化されると、機密保護コンポーネントの内部で既に第１の検査ステップの段階でそのような変化は確定され、機密保護コンポーネントは非動作状態とされるので、後続する検査ステップのためにその機密保護コンポーネントを利用することは不可能になり、それらのステップを実行することはできなくなる。

第１図には、スーパーバイザリーコンピュータにおいてオブジェクトコンピュータのシステムサポータ及び機密保護コンポーネントが本発明による方法の下でどのような状態にあるかが示されている。垂直の破線の左側には、機密保護方法の枠内でアクティブであるスーパーバイザリーコンピュータのコンポーネントが示され、右側には、オブジェクトコンピュータへの導入のために準備されなければならないパッシブなコンポーネントが示されている。アクティブなコンポーネントは、検査暗号の計算のために実行されるべき個々の暗号化ステップを制御する暗号化プログラム11と、プログラムごとに１つの検査暗号を出力することができるように、暗号化プログラム11の制御の下

に機密保護すべきプログラムの供給を受ける暗号化コンポーネント12である。パッシブなコンポーネントは、機密保護されるプログラムに関する検査暗号記憶装置14及びクリアテキスト記憶部13を有するシステムサポータ15と、機密保護コンポーネント16と、事前ローダプログラムに関するクリアテキスト記憶装置17である。

オブジェクトコンピュータへの導入のために、パッシブなコンポーネントを準備するときには、まず、暗号化プログラム11の制御の下に、クリアテキスト記憶装置17から事前ローダプログラムが取出され、暗号化コンポーネント12により、このコンポーネントにあらかじめあった秘密キーを使用して、その事前ローダプログラムに対応する検査暗号が計算される。この暗号は暗号化コンポーネント12から出力され、暗号化プログラム11の制御の下に機密保護コンポーネント16に供給される。このステップと同時に、機密保護コンポーネント16には、読出し保護記憶のための秘密キーが受け渡される。その後、システムサポータ15のクリアテキスト記憶部13に記憶されているプログラムに関する検査暗号が計算され、暗号化プログラム11の制御の下にシステムサポータ15の検査暗号記憶装置14に記憶される。スーパーバイザリーコンピュータの暗号化コンポーネント12において実行される全ての暗号化ステップの基礎となるのは、暗号化コンポーネント12に記憶されている秘密キーである。

第2図は、上述のように準備されたシステムサポータ及び機密保護コンポーネントがオブジェクトコンピュータにおいて一般にどのような方式でプログラムの保全制御に適用されるかを示す。オブジェクトコンピュータのシステム始動段階の中に位置することができる一連の検査ステップの一部として1つの検査ステップが示されている。垂直の破線の左側にはオブジェクトコンピュータのアクティブなコンポーネントを示し、右側にはパッシブなコンポーネントを示す。それぞれの検査ステップは、チェッカーと呼ばれ、検査目的物、すなわち検査されるべきプログラム23及び付属する検査暗号24を機密保護コンポーネント22に供給する検査実行プログラム21により実行される。前述のように、機密保護コンポーネント22は供給されるプログラムごとに、このコンポーネントに入力された秘密キーを使用して検査暗号を計算し、これを先に供給された付属検査暗号24と比較する。機密保護コンポーネント22は、検査実行プログラム21の制御の下に、イエス／ノーステートメントの形をとる比較の結果を次の検査実行場所へ引き渡すが、ステートメントがイエスである場合には、この場所はたった今検査されたばかりのプログラムということになる。ステートメントがノーであれば、誤り状況を信号により報知することができ、たとえば、システムのプロセスを中断するか、誤り警報を発信するか、又はその他の方法により修正措置を強行する特別の機能ブロックが活動状態とされる。

以上説明したプロセス全体は、検査実行プログラム21に供給されるスタート信号により開始される。この信号は先行する検査ステップのイエスのステートメントであるか、又はシステム始動のための最初のスタート信号であることができる。

第3図は、前述のような種類の一連の検査ステップがオブジェクトコンピュータにおいていかにして実行されるかを示す。ここでは、それらの検査ステップの時間的な流れを示しており、ステップは上から下に向かって3つの段階、すなわち、スイッチオン段階と、システム始動段階と、応用段階とに分割されている。この場合にも、第1図及び第2図と同様に、垂直の破線の左側にはアクティブなコンポーネントが示され、右側にはパッシブなコンポーネントが示されている。個々の検査ステップは順にＳ０，Ｓ１，Ｓ２，Ｓ３…Ｓｎの符号で示される。それぞれの検査ステップＳ１からＳｎにおいて、アクティブなコンポーネントとして検査実行プログラムが示され、パッシブなコンポーネントとして検査されるべきプログラムが示されている。それぞれの検査ステップの機密保護コンポーネントは、その機能について既に第2図を参照して説明したので、ここには図

示されていない。

オブジェクトコンピュータのスイッチオンに伴なって、検査ステップＳ０においてスタート信号ＳＴが事前ローダプログラム31に印加される。事前ローダプログラム31はこの信号により制御されて、検査ステップＳ１を開始させる。この検査ステップＳ１がシステム始動段階の第１のステップとなる。検査ステップＳ１において、事前ローダプログラム31は検査されるべきプログラムとして機密保護コンポーネント35に供給され、このコンポーネントでは、記憶されている秘密キーを使用して検査暗号の検査のための暗号化が実行される。次に、この検査暗号は、機密保護コンポーネント35に記憶されていた事前ローダプログラム31に関する検査暗号と比較される。２つの検査暗号が一致した場合はイエスのステートメントが発生され、それにより、検査ステップＳ２について事前ローダプログラム31が導入されるので、この事前ローダプログラムはこの検査ステップに関して、常駐オペレーティングシステム32を検査するためのアクティブコンポーネントとなる。機密保護ブロック35から発生されるノーのステートメントは制御プログラム36に供給され、この制御プログラム36はこれ以降のシステム動作を図示されない方法により中断することができる。

常駐オペレーティングシステム32はパッシブなコンポーネントとして、個々のプログラム部分を伴なって、事前ローダプログラム31によりこの検査ステップＳ２については図示されていない機密保護コンポーネントに渡されて、そこで暗号化を受けることができ、その結果、検査暗号が発生される。この検査暗号は、同時に事前ローダプログラム31に、又はそれと結合している機密保護コンポーネントに供給される検査暗号34と比較される。２つの検査暗号が同じであるときに発生されるイエスのステートメントは常駐オペレーティングシステム32を制御して、これをアクティブなコンポーネントにし、そこで、常駐オペレーティングシステムはロードライブラリー33からのプログラム部分の検査を開始させる。この検査ステップＳ３は検査ステップＳ２と同様に実行されるので、そこで計算された検査暗号がそれぞれ検査されるべきプログラムに付随する検査暗号34と一致する場合は、イエスのステートメントが発生され、このステートメントは制御プログラム36に送られる。そこで、制御プログラム36は応用段階の動作を信号ＡＷにより開始させることができる。

応用段階の中では、スーパーバイザリーコンピュータにおいて個々のアプリケーションプログラムが検査暗号記憶装置又はロードライブラリーに記憶可能である検査暗号を備えている限り、当然のことながら、ここで説明した態様の検査ステップをさらに実行することができる。

第４図には、スーパーバイザリーコンピュータにおける暗号化コンポーネントによる検査暗号の発生がブロック線図で示されている。検査暗号ＰＺ（ＰＯ）を計算しなければならない検査すべきプログラム、すなわち検査対象物は、アドレスＡＤＲ及び長さＬＡＥを与えられながら、検査対象物を個々のブロックＢに分割するための分割プログラムに供給される。これらのブロックＢは互いに等しい長さを有し、それぞれ少なくとも１回は、秘密スタート値ＳＷ及び秘密キーＩＫを伴なうＤＥＳ暗号化ステップの実行を受ける。このとき、暗号化プログラム41が利用される。それぞれ１つのブロックＢの暗号化に際して発生する結果Ｃは、次に暗号化すべきブロックのためのスタート値として暗号化プログラム41に供給される。最終ブロックＢの暗号化の結果はＣＥで表わされ、ある１つのプログラムに対応するか、又は機密保護コンポーネントにおいて事前ローダプログラムに関する検査暗号として記憶されることができる発生検査暗号ＰＺ（ＰＯ）である。

なお、このような検査暗号の発生はファームウェア又はソフトウェアのいずれによっても実行可能である。

第５図は、機密保護コンポーネントを有するオブジェクトコンピュータにおける検査暗号制御の実行を示す。検査暗号制御は、入出力パラメータと、比較プロセスとに関してのみ、第４図を参照

して説明した発生と異なる。補助的な入力パラメータは、検査暗号ＰＺ（ＰＯ）の計算後に比較値として使用される基準値ＲＷである。比較の結果は、既に説明したように、イエス／ノーのステートメントとして、後続する検査ステップ又は制御プログラムを開始させる。

検査暗号制御の方法は、第４図に示される暗号化及び第５図に示される検査暗号制御について暗号化プロセス、スタート値及びキーの一致を必要とする。

第６図は、一実施例として、機密保護コンポーネント60の原理的構成を示す。ここでは、差込み接続部を介してオブジェクトコンピュータに接続することができるハードウェアモジュールに関して説明する。この接続部を介して命令及びデータはオブジェクトコンピュータと、機密保護コンポーネントとの間で交換される。機密保護コンポーネントの基本的な構成要素はプロセッサ61と、機密保護ハイブリッドモジュール62である。プロセッサ61は、たとえば、命令コード化、データ線の接続及び機密保護ハイブリッドモジュール62への指令受け渡しのために、機密保護コンポーネント60の個々の機能を制御する。機密保護ハイブリッドモジュールは集積回路の態様による構成要素であるが、そのモジュール構成要素は別箇に取付けられており、その全体にセラミックカバーを設けることができる。ハイブリッドモジュールはプロセッサ63と、ＤＥＳ素子64と、選択的にアクセス可能な２つのキー記憶装置65及び66とを含む。プロセッサ63はＤＥＳ素子64と、設出し保護されたキー記憶装置65及び66との間の命令及びデータの制御と実行のためのものである。さらに、プロセッサ63はプロセッサ61への外部データ流れを制御する。ＤＥＳ素子64は上述の暗号化方式を制御する。キー記憶装置65は、ＤＥＳ暗号化のために利用される、たとえば64ビットの長さのキーを受入れ、キー記憶装置66は、プロセッサ63により内部機能のためにのみ利用されることができ、外部アプリケーションプログラムによる利用は不可能であるキーを記憶する。機密保護ハイブリッドモジュールの内部の１本のデータ線に対するアクセスは、前記セラミックカバーにより阻止される。機密保護コンポーネント60からオブジェクトコンピュータへの接続が遮断されてしまうと、それにより、キー記憶装置65は消去される。キー記憶装置66の内容については、バッテリーによりこれを保持することができる。ハイブリッドモジュール62が機密保護コンポーネント60から取外されると、全ての記憶値は失なわれることになる。これにより、コンピュータ領域の外側で機密保護コンポーネント60を利用することは不可能であるという状況が保証される。

4．図面の簡単な説明

第１図は、本発明の方法を実施した場合のスーパーバイザリーコンピュータのコンポーネントの相互対応及び相互交換作用を示す図、

第２図は、本発明の方法を実施した場合のオブジェクトコンピュータのコンポーネントの相互対応及び相互交換作用を示す図、

第３図は、オブジェクトコンピュータにおける連続する検査ステップの経過を示す図、

第４図は、スーパーバイザリーコンピュータの暗号化コンポーネントにおける検査暗号形成を伴なう暗号化の原理プロセスを示す図、

第５図は、オブジェクトコンピュータの機密保護コンポーネントにおける暗号化及び検査暗号比較の原理プロセスを示す図、及び

第６図は、機密保護コンポーネントの基本構成を示す図である。

11…暗号化プログラム
12…暗号化コンポーネント
13…クリアテキスト記憶部
14…検査暗号記憶装置　15…システムサポータ
16…機密保護コンポーネント
17…クリアテキスト記憶装置
21…検査実行プログラム
22…機密保護コンポーネント
23…検査されるべきプログラム
24…付属検査暗号

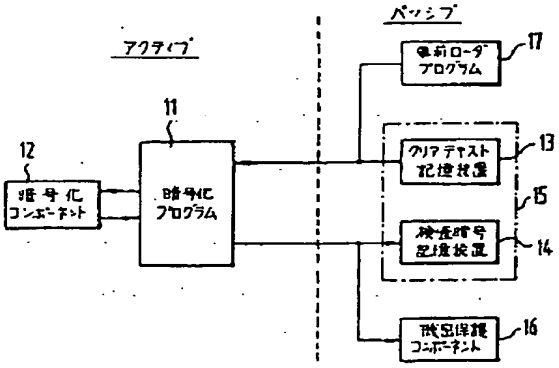

FIG. 1

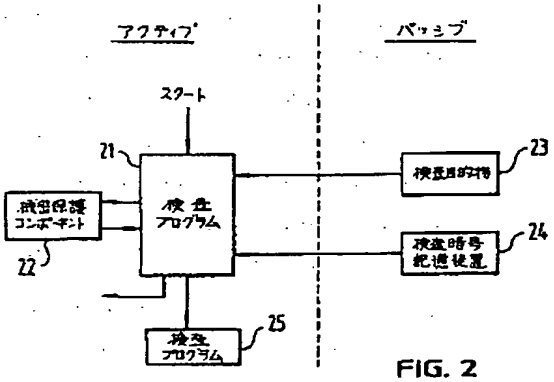

FIG. 2

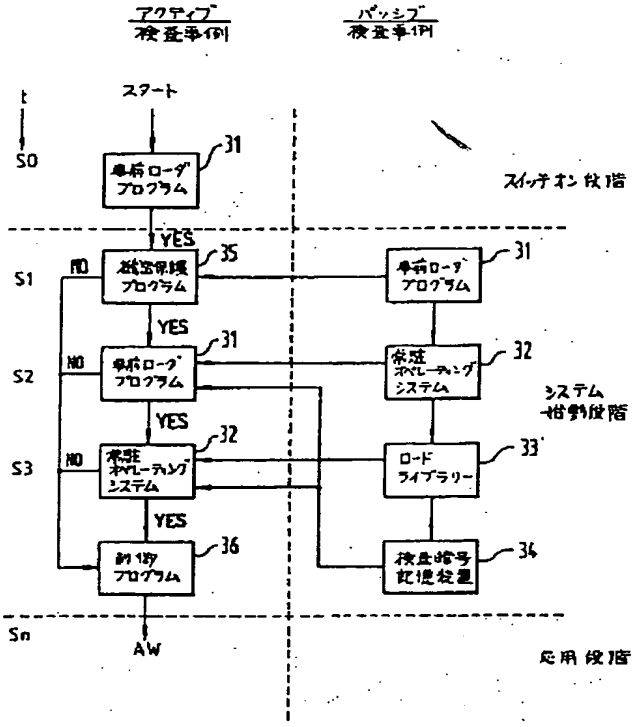

FIG. 3

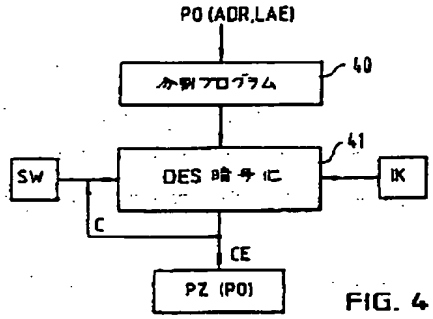

FIG. 4

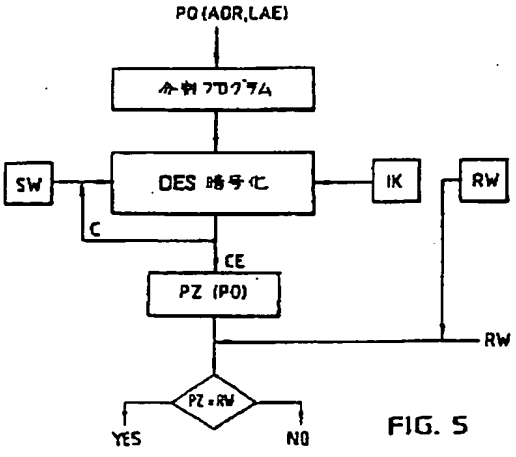

FIG. 5

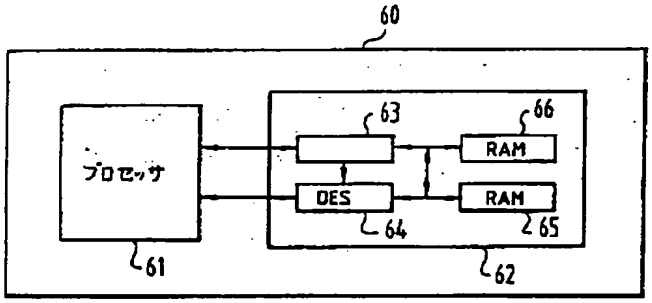

FIG. 6